IS 15296 (2003): Industrial Automation Systems - Safety of Integrated Manufacturing Systems - Basic Requirements [PGD 18: Industrial and Production Automation Systems and Robotics]

BLANK PAGE

IS 15296 : 2003
ISO 11161 : 1994

भारतीय मानक

औद्योगिक स्वचालन तंत्र – समेकित निर्माण तंत्रों की सुरक्षा–आधारभूत अपेक्षाएँ

Indian Standard

INDUSTRIAL AUTOMATION SYSTEMS — SAFETY OF INTEGRATED MANUFACTURING SYSTEMS — BASIC REQUIREMENTS

ICS 25.040.30

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

February 2003 **Price Group 10**

NATIONAL FOREWORD

This Indian Standard which is identical with ISO 11161:1994 'Industrial automation systems—Safety of integrated manufacturing systems—Basic requirements' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendation of the Industrial and Production Automation Systems Sectional Committee and approval of the Basic and Production Engineering Division Council.

The text of the International Standard has been approved as suitable for publication as Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker in the International Standard while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to the following International Standard for which Indian Standard also exists. The corresponding Indian Standard which is to be substituted in its place is listed below along with its degree of equivalence for the edition indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
IS/TR 8373:1988[1)] Manipulating industrial robots—Vocabulary	IS 14662:1999 Industrial robots—Vocabulary	Modified[1)]

Where there are no corresponding Indian Standards for the International Standards referred in this Indian Standard, reference to the relevant International Standard may be made.

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis shall be rounded off in accordance with IS 2:1960 'Rules for rounding off numerical values (*revised*)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

[1)] ISO/TR 8373 is revised as ISO 8373:1994 and IS 14662:1999 is identical to ISO 8373:1994.

Introduction

0.1 This International Standard is part of a series of standards dealing with safety of industrial machines. It has been harmonized with other relevant International Standards dealing with safety issues of industrial equipment.

The intent of this International Standard is to provide safety requirements and guidelines for the design, construction, installation, programming, operation, use, and maintenance of integrated manufacturing systems. It describes basic types of hazards associated with these systems and steps to be taken to assess the risks associated with these hazards and to eliminate or reduce the hazards to an acceptable level.

Where specific points in this International Standard are considered to be in conflict with the requirements of other international standards (now or in the future), these requirements will be analysed to determine if they are to be included or deleted as system safety requirements.

0.2 This International Standard has been created in recognition of the particular hazards which exist in integrated manufacturing systems incorporating industrial machines and associated equipment.

The risks associated with these hazards vary with the types of industrial machines incorporated in integrated manufacturing system and the application of such a system as to how it is installed, programmed, operated, maintained and repaired.

The requirements of this International Standard are aimed at minimizing the possibilities of injuries to personnel while working on or adjacent to an integrated manufacturing system. This International Standard contains definitions, measures or procedures, and devices which are not specific to systems but can also apply to safety requirements for individual machines and equipment. They are included in this International Standard to make it more understandable or because no relevant international standards exist.

Figure 0.1 shows a typical system with the assumption that all of the hazards presented by the system are contained within the work zone. These hazards are suitably protected by safeguarding means determined by the risk assessment (see clause 4) and described in clauses 5 to 8 of this International Standard.

Where hazards are presented by equipment outside the work zone (e.g. electrical shock), it is intended that these hazards be suitably protected by means described in relevant International Standards (e.g. IEC 204-1) which can be integrated by the procedures developed by the system supplier or user.

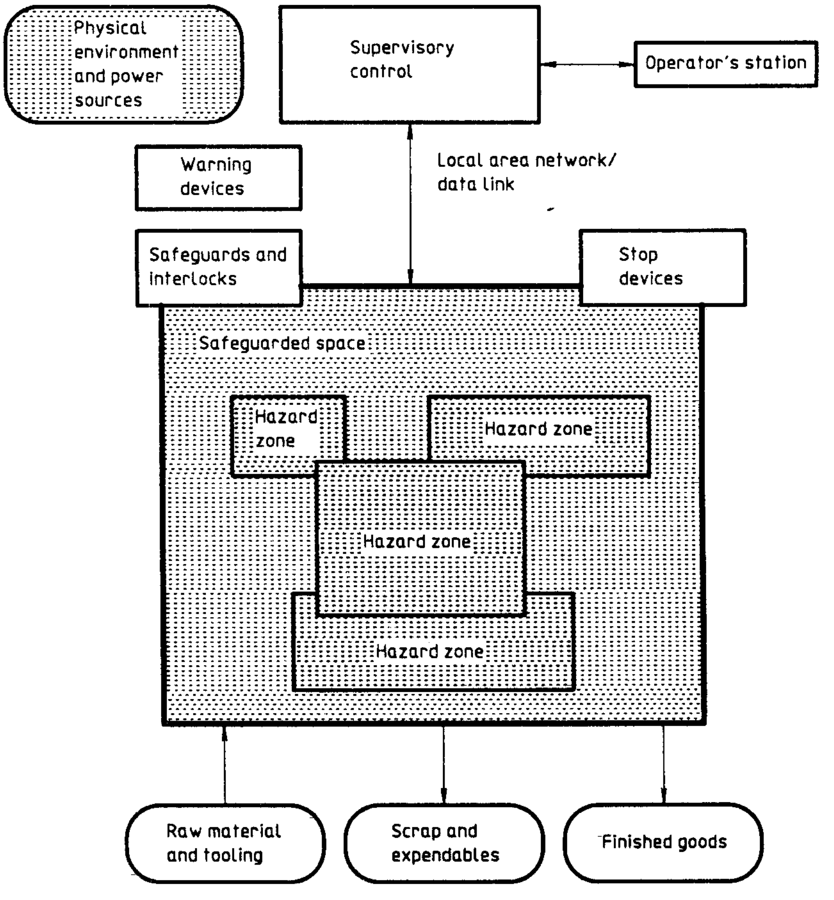


Figure 0.1 — Basic integrated manufacturing system

Indian Standard

INDUSTRIAL AUTOMATION SYSTEMS — SAFETY OF INTEGRATED MANUFACTURING SYSTEMS — BASIC REQUIREMENTS

1 Scope

This International Standard specifies the safety requirements for integrated manufacturing systems that incorporate two or more industrial machines interconnected with and operated by a controller(s) capable of being reprogrammed for the manufacturing of discrete parts or assemblies. It describes the requirements and recommendations for the safe installation, programming, operation, maintenance, or repair of such systems (see figure 0.1 for the basic configuration of an integrated manufacturing system).

This International Standard is not intended to cover safety aspects of individual machines and equipment which may be covered by standards specific to those machines and equipment. Where machines and equipment of an integrated manufacturing system are operated separately or individually and while the protective effects of the safeguards provided for automatic mode are muted or suspended, the relevant safety standards for these machines and equipment shall apply.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 3864:1984, *Safety colours and safety signs.*

ISO 6385:1981, *Ergonomic principles in the design of work systems.*

ISO/TR 8373:1988, *Manipulating industrial robots — Vocabulary.*

ISO 10218:1992, *Manipulating industrial robots — Safety.*

CEI 204-1:1992, *Electrical equipment of industrial machines — Part 1: General requirements.*

EN 418:1992, *Safety of machinery — Emergency stop equipment, Functional aspects — Principles for design.*

3 Definitions

For the purposes of this International Standard, the following definitions apply.

3.1 awareness barrier: Attachment or obstacle that by physical contact warns of an approaching or present hazard.

3.2 barrier: Physical boundary to a hazard.

3.3 controlled stop: The stopping of machine motion by reducing the command signal to 0 once the signal has been recognized by the control but retaining power to the machine actuators during the stopping process. [IEC 204-1:1992, 3.12]

3.4 enabling device: Manually-operated device which, when continuously activated in one position only, allows hazardous functions but does not initiate them. In any other position, hazardous functions are stopped safely.

3.5 guard: Machine element specifically used to provide protection by means of a physical barrier. Depending on its construction, a guard may be called casing, cover, screen, door, enclosing guard, etc.

3.6 hazard: Source of possible injury or damage to health.

3.7 hazard zone [area] [space]: Any zone within and/or around machinery in which a person is exposed to risk of injury or damage to health.

3.8 hazardous situation [condition] [motion]: Any situation in which a person is exposed to a hazard or hazards.

3.9 hold-to-run control device: Manually-actuated start and stop control device which initiates and maintains operation of machine elements only as long as the control is actuated in a set position. The control automatically returns to the stop position when released.

3.10 industrial machine; machine: Individual component machine and associated equipment of an integrated manufacturing system.

3.11 integrated manufacturing system; system: Group of two or more industrial machines working together in a coordinated manner normally interconnected with and operated by a supervisory controller or controllers capable of being reprogrammed for the manufacturing of discrete parts or assemblies.

3.12 interlocking device (as used with a guard): Mechanical, electrical, or other type of device, the purpose of which is to prevent the operation of system elements under specified conditions (generally as long as the guard is not closed).

3.13 limiting device: Device which prevents a system or system elements from exceeding a design limit.

3.14 local control: State of the system or portions of the system in which the system is operated from the control panel or pendant of the individual machines only.

3.15 lockout: Placement of a lock on the energy isolating device (e.g. disconnecting means) in the "OFF" or "OPEN" position indicating that the energy isolating device or the equipment being controlled shall not be operated until the removal of the lock.

3.16 muting: Temporary automatic suspension of the protective function of a safeguarding device during normal operation.

3.17 operational stop: Stop which stops the production process at a natural point in the working process as soon as possible after its activation.

3.18 pendant: Unit linked to the control system with which the system or portions of the system can be programmed (or moved).

3.19 person: Any individual.

3.20 personnel: Persons specifically employed and trained in the use and care of a machine or manufacturing system.

3.21 protective device: Device (other than a guard) which reduces risk, alone or associated with a guard.

3.22 risk: Combination of the probability of injury occurring and the degree of the injury or damage to health in a definite hazardous situation.

3.23 safeguard: Guard or protective device used in a safety function to protect persons from a present or impending hazard.

3.24 safeguarded space: Space determined by the safeguards.

3.25 safeguarding: Those safety measures consisting of the use of safeguards to protect persons from the hazards which cannot reasonably be removed or sufficiently eliminated by design.

3.26 safe working procedure: Specified procedure intended to reduce the possibility of injury while performing an assigned task.

3.27 supplier: Entity (e.g. designer, manufacturer, contractor, installer, integrator) who provides equipment or services associated with the manufacturing system or portion of the system.

NOTE 1 The user may also act in the capacity of a supplier to himself.

3.28 task program: Set of motion and auxiliary functions instructions which define the specific intended task of the manufacturing system.

NOTE 2 This type of program is normally generated by the user.

3.29 trip device: Device which causes a system or system element to stop when a person or a part of his or her body goes beyond a safe limit.

3.30 troubleshooting; fault finding: Act of methodically determining the reason that the system or portions of the system has failed to perform the task or function as intended.

3.31 uncontrolled stop: Stopping of machine motion by removing power to the machine actuators which cause hazardous conditions, all brakes or other mechanical stopping devices being activated (see IEC 204-1).

3.32 user: Entity who utilizes and maintains the manufacturing system.

4 Safety strategy

4.1 General

This clause deals with the overall strategy of determining the safety requirements for a system. This overall strategy is a combination of the measures incorporated at the design stage and those measures required to be implemented by the user.

The design of the system shall be the first consideration while still maintaining an acceptable level of performance. This phase of the safety strategy should:

— specify the limits or parameters of the system (see 4.2);

— apply a safety strategy (4.3);

— identify the hazards (4.4);

— assess the associated risks (4.5);

— remove the hazards or limit the risks as much as practicable.

Where it is not possible to reduce the risks to an acceptable level by the above measures, provisions for safeguarding in the design phase shall be considered in such a manner that the flexibility of the system in its application is retained without impairing its safety.

In addition, information (e.g. written instructions, warning signs) concerning hazards which are difficult to recognize shall be provided.

4.2 System specification

A system concept shall define the system specification. This includes or takes into account:

— description of functions;

— layout and/or model;

— survey about the interaction of different working processes and manual activities;

— analysis of process sequences including manual interaction;

— description of the interfaces with conveyer or transport lines;

— process flow charts;

— foundation plans;

— plans for supply and disposal devices;

— determination of the space required for supply and disposal of material;

— available accident records;

— study of similar system installations.

The designer shall have a specific and documented idea of the probable human activities on the site, and in particular:

— visits (presence of third parties not directly concerned by the operation);

— process control and monitoring;

— workpiece loading;

— takeover of manual control by operator;

— brief interventions not requiring disassembly;

— setting;

— troubleshooting;

— maintenance.

This information will enable the designer to work out a coherent, purposeful programme of action based on the following elements:

— analysis of reference situations (old or more recent on other sites);

— allowance for effects of industrial variability (equipment wear, dimensional variations of product, etc.);

— participation of personnel having to work on the system in the future.

4.2.1 System design criteria

Besides the description of functions, all necessary requirements to ensure safe operation should be considered in the design criteria list. This includes all protective measures to effectively reduce the hazards listed in 4.4 where they exist.

Such a design implies a coherent procedure which minimizes the effects of project fragmentation. This requires:

— integration of the man-machine interface;

— early definition of the position of those working on the system (in time and space);

— early consideration of ways of cutting down on isolated work;

— consideration of environmental aspects (e.g. quality of air, lighting conditions, noise).

A system shall not be designed exclusively in terms of its working functions; it shall also be considered from the viewpoints of its use and operation.

4.2.2 Project organization

During planning, design and construction of a manufacturing system, safety measures especially those related to the interactions between individual machines shall be coordinated. This applies also where a system consists of a combination of sections and/or single units from different suppliers.

The coordination of activities include, for example:

— planning;

— procurement;

— delivery and assembly;

— installation procedure and stage of testing;

— partial acceptance/acceptance;

— delivery of the system in final working order;

— system verification (runoff) including correction of any faults or failures found;

— maintainability;

— ergonomic factors.

4.3 Application of a safety strategy

An integrated manufacturing system shall be designed and safeguarded to ensure orderly transport and installation as well as proper and safe use and maintenance in accordance with the risk assessment (see 4.5). To achieve these objectives the relationship between human factors, the work being carried out, the hazards arising and the production process should be taken into account.

The factors of noise, hazardous materials, heat, low temperature, radiation and similar influences of the physical operating environment shall be considered so as not to create health hazards.

The supplier(s) of the system (or parts of the system) shall state the expected conditions of the physical environment and the requirements of the external powers sources and how they are to be connected to ensure proper operation. The user shall ensure that either these conditions are met or that alternative means are provided and that the system operates under these conditions according to the specification.

4.3.1 Design and development

All available knowledge concerning safety should be considered during the development of single units, sections of system and complete systems so that, through its application, accident and health hazards shall be prevented or reduced to an acceptable level. This includes the clarity of the complete system, the sections of system and the single units. Particularly, the normal operating positions of personnel shall grant sufficient vision of the flow of production and the machining operations which may require additional measures (e.g. video monitoring).

Normal positions for operating and maintenance personnel shall be easily accessible and located outside hazardous areas. Elements requiring routine maintenance (e.g. points of lubrication, setting mechanisms) shall be arranged, where practicable, outside the hazardous areas. It is preferable to achieve the desired levels of safety by the use of nonhazardous elements to remove or reduce hazards. Secondly, alternative process sequences or working processes giving a lower level of risk may be used.

Manually-operated start and stop controls shall be located in such a way that the hazard zone which is associated with that control facility is clearly identified.

4.3.2 Safeguarding

Where the measures in accordance with 4.3.1 are not or only partially applicable in reducing risks to an acceptable level, the safeguards given in clause 6 shall be provided. These safeguards shall not complicate operation and maintenance more than necessary. This includes the clear arrangement in conjunction with the complete system, the sections of system and the single units.

Depending upon the design and application of the system, the use of a single safeguard or a combination of several different safeguards may be necessary. The selection of the safeguards depends upon the identified hazards.

Safeguarding means shall remain effective for all operating modes (see IEC 204-1:1992, subclause 9.2.4 for suspension of safeguards under special conditions).

4.3.3 Warning signs and personal protective equipment

Where the measures given in 4.3.2 and 4.3.2 are not or only partially applicable, warning devices (see 6.6) and signs shall indicate the presence of the remaining hazards which are difficult to recognize.

The following hazards can be difficult to recognize:

— those due to unexpected movements;

— those due to unexpected effects of energy (e.g. by overpressure, tension, rotation, gravity, noise, heat, low temperature, radiation); or

— those due to unexpected escape of hazardous materials.

Where necessary, the use of personal protective equipment shall be specified.

4.4 Hazard identification

Hazards can arise from

— the system itself;

— the interaction of the system with other machinery or equipment outside the system;

— the physical environment in which the system is used; or

— interactions between personnel and the system.

Examples of sources of hazards are:

a) moving mechanical components in

   1) normal operation either individually or in conjunction with other elements of the system or related equipment in the hazard zone,

   2) unexpected operation (e.g. falling of mechanical components, tipping of the machinery);

b) power sources;

c) stored energy;

d) interferences

   1) electrical [e.g. electromagnetic interference (EMI), electrostatic discharge (ESD), radio frequency interference (RFI)],

   2) mechanical (e.g. vibration, shock);

e) hazardous atmospheres or materials

   1) explosive or combustible,

   2) corrosive,

   3) radiation (e.g. ionization, thermal);

f) failure or fault of

   1) protective means including removal, disassembly, or defeating,

   2) components, devices, or circuits,

   3) power sources or means of power distribution including fluctuations or disturbances,

   4) information transmission;

g) human error

   1) design, construction, or modification,

   2) operating systems, application software, and programming,

   3) application and implementation,

   4) setup including work handling/holding and tooling,

   5) operation or use,

   6) maintenance and repair,

   7) documentation and training/instruction;

h) ergonomic considerations

   1) lighting,

   2) vibration,

   3) noise,

   4) climatic conditions,

   5) operator control station design/layout.

4.5 Risk assessment

A risk assessment shall be performed which shall serve as a basis for determining safety objectives and measures.

Risks shall be reduced to an acceptable level. To achieve this requirement, it is the intent of this subclause to provide guidance in the development of programs or plans to

— create a safe working environment, and

— ensure safety and health of personnel.

Each identified hazard shall be assessed for its risk and appropriate safety measures shall be determined and implemented to minimize that risk.

Hazards shall be ascertained for the single units, the interaction between single units, the operating sections of the system, and operation of the complete system for all intended operating modes/conditions including conditions where normal safeguarding means are suspended for such operations as programming, verification, troubleshooting, maintenance, or repair. This also applies where systems are modified.

Risks shall be evaluated for normal operation where conditions are clearly foreseeable including the interaction of personnel as part of the production process. Where a hazard exists, normal production should avoid human intervention.

Risks shall also be considered for those parts of the process where it is foreseeable that there will be direct human intervention within the system (e.g. clearing blockages, setting, programming/teaching, troubleshooting, maintenance). It should be recognized that under these circumstances the normal control sequences and some or all of the normal process safeguards may be suspended. Where this is the case, special provisions should be made for local control and safeguarding together with dedicated safe systems of work (e.g. lockout).

The hazardous situations which can occur in each area of the system to which persons can have access, shall be identified.

4.6 Ergonomic considerations

4.6.1 Man-machine interface

The following measures are designed to facilitate the activities of automated system monitoring and data processing.

4.6.1.1 Direct view of operations

The site shall be designed to facilitate the acquisition of information concerning sensitive points of the system; special attention shall be paid to the layout of observation points or areas (it may be useful to provide for viewing aids such as mirrors, video systems, etc.).

4.6.1.2 Information displayed

The user shall be able to obtain all necessary information concerning the actual state of the progress of the operating cycle. Comprehensive information concerning the state of the system should be available on the man-machine interfaces. Special attention shall be paid to the choice of information to be displayed on these interfaces and information which can be accessed by the system operator on request.

This information shall be presented in a language which takes into account the customary activity and technical culture of the system operators. For information display, the conditions listed below concerning its form and appearance shall be complied with

— the physical characteristics of signals and controls shall be adapted to the viewing and manipulating capabilities of all operators;

— the controls and information relating to a given action and monitoring of its result shall be located close to one another;

— the grouping of information shall promote diagnosis (i.e. facilitate the identification of significant configurations of the technical system);

— information allowing verification of the reliability of an indicator shall be located close to that indicator;

— the conventions adopted shall be the same for all devices (colours, abbreviations, direction of scrolling, orientation of diagrams, etc.). Importance of identifying labels (see also IEC 204-1);

— the design of display systems shall be such as to allow detection of display-system malfunctions and repair of the system;

— allowance shall be made for the capability of the device to evolve with evolutions in production, user population, etc.;

— duplication: it is often necessary for the same information to be displayed at several locations on the site.

At the site design stage, consideration shall be given to the possibility of the users storing in memory significant events (settings, oil changes, drifts, contingencies, incidents). Storage in memory should make it possible for the user to trace the history of the system.

In addition, the information conveyed via several interfaces shall be interconnected to ensure the coherence of such information, especially when the principle of redundancy is employed.

4.6.1.3 Manually-operated control devices

The design and location of manually-operated control devices should:

— ensure that the state of each power actuated device is visible from the position of the manually-operated control device;

— ensure that functions and statuses are defined and displayed explicitly for the operator;

— harmonize the manually-operated control devices (e.g. designation, positions) by ensuring consistency between the various control parts of a given system;

— adapt the shapes and sizes of the actuators of the control devices to ensure that they can be actuated without error by workshop operators.

The effects of the actuation of any manually-operated control device shall be clearly defined. The state of the actuated control device shall be made clearly apparent.

4.6.2 Human interventions

4.6.2.1 Control and maintenance activities

Interventions areas shall be sized and arranged so as to provide sufficient space for movement and for performing the necessary tasks with minimum risk.

Provisions should be made, in particular, for

— areas for movement by those working on the system, avoiding, insofar as practicable, changes of levels and lengthy movements, and with provision for crossover points;

— a working space or platform for all long, frequent, or high-elevation interventions which takes into account the aspects of posture, body dimensions, the environment, and task;

— layout of interfaces, central and decentralized consoles (stationary or mobile) in such a way as to allow viewing of the part actuated, to limit time constraints and minimize risks related to faults in communication between operators;

— a lighting level in work areas and for parts of the site requiring special monitoring which is appropriate for the operations to be performed. Care should also be taken that visibility is not disturbed by phenomena such as glare or reflections. In certain cases, provisions should be made for the possibility of lighting adjustment (intensity, orientation);

— lifting bolts or other devices built into the equipment and/or forming part of the site and the use of special handling facilities to facilitate the assembly/disassembly of the system.

4.6.2.2 Predominantly manual activities

Application of ergonomic measures and data contributes to improvement of the safety level by making task completion easier and by decreasing the number of human errors during interventions (e.g. repairing, maintenance, checking, programming, operating). The design of system elements on which human intervention is intended shall take into account human characteristics such as size, posture, strength, movements, and physical ability (ISO 6385).

Care should be taken to ensure the operators

— maintain normal body position;

— can communicate (visually and orally).

4.7 Marking

The system shall be provided with a specific identification with the following information (as a minimum):

— name and location of manufacturer/supplier;

— system identifier;

— appropriate certification (where required).

4.8 Requirements for documentation

The system documentation shall be written in the language(s) agreed between the user and the supplier prior to the acceptance of the order and contain (as a minimum) the following:

a) a clear, comprehensive description of the system and its installation including mounting and connection to external energy sources;

b) a repetition of the markings found on the system (see 4.7);

c) the system performance specifications;

d) external power source(s) specifications;

e) physical environment specifications (e.g. lighting, vibration, and noise levels, atmospheric contaminants);

f) a description of potentially hazardous conditions and how to avoid them (e.g. lockout, blocking, pinning);

g) how to recognize abnormal performance and how to correct it;

h) information on the

   1) programming,

   2) operation,

   3) frequency of inspection,

   4) frequency and method of functional testing, and

   5) guidance on the repair and maintenance of the system and its safeguards;

i) a recommended procedure for maintaining a record of the task program to assist personnel in operating or troubleshooting;

j) a description (including interconnecting diagrams) of the safeguards, interacting functions, and interlocking of guards with hazardous movements particularly with interacting installations;

k) a description of the safeguarding means and methods when the primary safeguards are suspended;

l) a description (including diagrams) for the interfaces for the connection of control and power circuits;

m) procedures for adjustment of the limiting devices.

The instruction manual for a system shall include the various specific manuals for its component parts.

5 Design requirements for safety functions of the control system

5.1 General

The following requirements apply to the control aspects (e.g. electrical, hydraulic, pneumatic, mechanical) of integrated manufacturing systems.

Control systems shall be designed and constructed in a manner that they cause no hazards to persons when they are used according to their specification during normal operation (see 8.3) or manual operation (see 8.4). This applies also to the interaction between a complete control system with separate unit control systems in addition to unit control systems in relation to each other.

The electrical equipment of a system shall be in accordance with IEC 204-1:1992 and in particular clause 9.

The electrical power supply and the connection of the earthing (grounding) conductor shall be in accordance with the supplier's recommendations.

5.2 Interferences

The design and installation of the system shall incorporate good engineering practices which protect controls and control systems from sources of interference. If risks may be foreseen as a result of interference, then separate safeguards are required to ensure that interference with control functions does not present risks whenever the machines are put to their intended tasks.

Examples of sources of interferences include:

— electromagnetic interference (EMI);

— electrostatic discharge (ESD);

— radio frequency interference (RFI);

— vibration/shock;

— airborne noise;

— light;

— radiation.

5.3 Limitation of fault effects for safety functions

The control system shall be designed, constructed, and installed or applied to ensure that a single control component failure within the system does not prevent stopping action from taking place but will prevent initiation or successive system cycles from occurring until the failure has been corrected.

This requirement does not apply to those components whose failure cannot cause hazardous conditions.

When analysing faults, the following shall be considered (see figure 1):

— a single fault shall not give rise to any situation hazardous to persons;

— a first fault which has not been recognized in conjunction with a further fault (second fault) shall not give rise to any situation hazardous to persons.

It is assumed that two independent faults do not appear at the same time, but the designer shall take into account common mode failures.

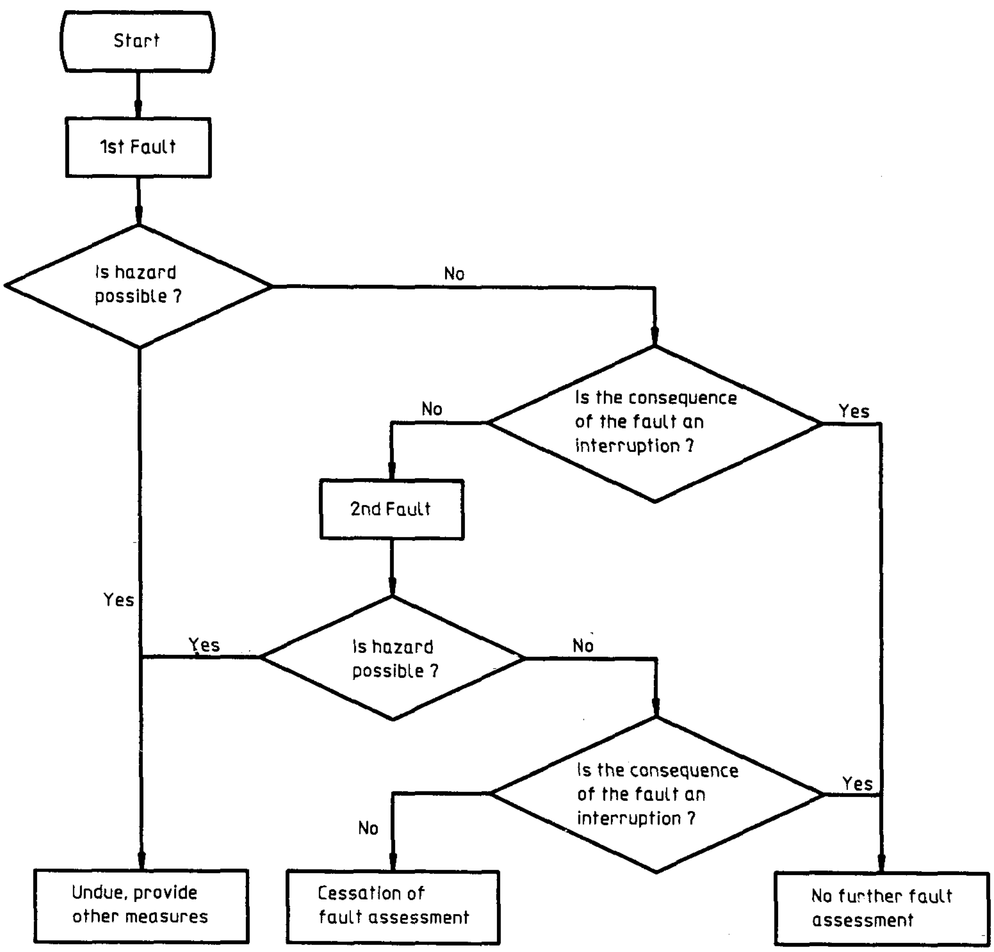


Figure 1 — Fault assessment

Failure consideration shall be made to maintain the safety-technical requirements in the case of failure and/or to ensure a detection of certain types of failures. Consequently, the development and assessment (fault analysis) shall be based upon assumption of the failure modes of the different components.

5.4 Safety measures

5.4.1 Safety measures by the control

In addition to the requirements of 5.3, proven circuit techniques and components (see IEC 204-1:1992, subclause 9.4.2.1) shall be used together with one or more of the following examples of safety measures:

a) Partial or complete redundancy (see IEC 204-1:1992, subclause 9.4.2.2).

   Control component failure protection of electrical, electronic or fluidic systems frequently consists of multiple, independent parallel or series circuitry or components arranged to meet the requirements of this subclause. Protection against the consequences of failure of control components should not depend solely upon simple redundancy.

   Component redundancy is the use of two or more control components in parallel or series circuits and is used to ensure reliable operation. However, failure of one of the redundant components can go undetected, allowing the appearance of safe operation. When the additional element(s) of the redundant circuit subsequently fails, an unsafe condition can occur. Monitoring and response to such single failures is essential;

b) Use of diversity (see IEC 204-1:1992, subclause 9.4.2.3).

c) Reduced speed (or power) of hazardous movements.

   The application of this measure assumes that a person can withdraw in time from a hazard coming from hazardous movements. This can be assumed if the reduced speed does not exceed 15 m/min in case of hazardous movements without a crushing or shear hazard (due to pushing) and it does not exceed 2 m/min in case of hazardous movements with a crushing or shear hazard. These values also apply if an enabling device is used at reduced speed;

d) Monitoring of control functions providing safety measures.

   The application of this measure (can also be carried out by simulation) assumes that monitoring carried out in a positive mode at fixed intervals determines how a consideration of the risk assessment will recognize an occurred fault and, in case of a recognized fault, will induce a safety signal (most of the time a shut-off signal);

e) Enabling device (see 6.5).

   The application of this measure assumes that the person who uses the enabling device will recognize hazards in time to take immediate steps to avoid them;

f) Delockable non-return valves, cyclic switching of slide valves which are infrequently actuated, force actuated valves, impulse valves without spring actuation.

   Considerable energies can be stored in hydraulic or pneumatic systems. It shall be assured that these do not lead to hazardous movements. Stored energies may be suited to induce safety functions (e.g. through restoring movements). If necessary additional measures shall be provided against later hazardous movements (e.g. due to drop in pressure, mains isolation, leakages, line breaks) such as, for example, mechanical force locked or positively located supporting facilities or delockable non-return valves.

5.4.2 Additional safety measures

Where safety measures by the control alone are not sufficient to protect against hazardous fault effects, complementary measures such as mechanical safety precautions shall be taken.

5.4.3 Combination of safety measures

Usually, a combination of safety measures are required. The safety measures to be taken shall be determined during the design of the control system for each component of the integrated manufacturing system which has to fulfil safety functions and by means of risk assessment (see 4.5). Where a combination of system components causes new safety requirements, these shall be solved at the system level.

5.5 Manually-operated control devices

Manually-operated control devices shall be readily visible, identifiable and appropriately marked or labelled. Those related to safety measures shall be positioned for safe operation without hesitation, loss of time, or ambiguity. These shall be located outside the hazard zone except for certain devices (e.g. emergency stop device, enabling device) when required as part of the safety measures.

5.6 Status indicators

Status indicators, where provided, shall indicate the operating condition of the system or a particular zone within the system.

5.7 Selection of the operating modes of the system

The control equipment shall have provisions for at least the following operating modes:

— normal (production) mode: all normal safeguards connected and operating;

— operation with some of the normal safeguards suspended;

— operation in which system or remote manual initiation of hazardous situations is prevented (e.g. local operation, isolation of power to or mechanical blockage of hazardous conditions).

The means for selection of operating modes shall be capable of being supervised for certain operations (e.g. programming, verification, maintenance). Where these operating conditions can present hazardous situations, interlocked access to the hazard zone(s) shall be required.

5.8 Control measures for the suspension of safeguards

Controls shall be designed in such a way that where

— setup [see 8.4.2 a)];

— programming [see 8.4.2 a) and 8.5];

— program verification [see 8.4.2 b) and 8.6];

— troubleshooting (fault finding, observation of production cycles) [see 8.4.2 b) and 8.7];

— maintenance [see 8.8]

cannot be performed from outside the safeguarded space, the relevant safeguards may be suspended to allow personnel to enter the hazard zone. The suspension of those safeguards should preferably be time limited (e.g. 10 s). The suspension may be by a lockable selection device or by other devices with an equivalent level of safety.

A sufficient level of safety can be achieved by other measures than lockable selection device only.

When personnel are required to be in the hazard zone, the following safety measures shall be provided in the control system in accordance with the requirements of clause 8:

— hold-to-run;

— enabling device;

— reduced speed;

— reduced power;

— portable emergency stop.

When safeguards are suspended as above, it shall not be possible for a hazardous situation to be initiated from outside the hazard zone.

Normal production shall only be possible when the protective effects of safeguards are reestablished.

To assist operating personnel during the suspension of safeguards, consideration shall be given to providing aids. The aids may include

— indication of the status of safety related functions/circuits and actuators which can cause hazardous conditions;

— indication of conditions of essential elements (e.g. status of work in progress, parameters such as position of elements of the equipment, temperature).

5.9 Local operation

Where local operation of the equipment in a hazard zone is provided, the remaining portion of the system shall be notified of this condition. Means for the selection of local operation shall be designed and constructed to allow the system operator or others in a particular zone to locally operate equipment within that zone but prevent any external means from actuating any equipment within the zone while the zone is under local operation.

Where a system or zone is provided with local operation, the means for selection shall be:

— located outside the hazard zone; and

— capable of being controlled by the operator or other designated personnel (e.g. key lock switch or access code).

Machines and related equipment in local operation shall be under the direct control of the system operator. No hazardous conditions may be actuated from a remote or external location when under local control.

Switching between local and remote or external operation shall not by itself create any hazardous situations.

5.10 Starting

It shall be possible to start the system, or machines and related equipment within operating zones of the system, from a control station located outside the associated protected zone provided that all safeguards associated with that zone are in place and functional, and all normal operating conditions have been met.

When it is required that the system (or a particular zone) be started concurrently from several control stations, these starting means shall be interlocked to prevent starting from less than the required number of stations.

Conversely, when for reasons of safety, a particular zone of the system is to be started from a single point of control, the other start controls shall be so designed and implemented to prevent starting of other zones of the system or that zone of the system from other locations.

5.11 Stopping

Each system or zone within the system shall have, as a minimum requirement, provisions for two levels of stopping; one related to safety measures and the other related to normal operating conditions. Normal operating conditions includes safety measures. The implementation of the stopping functions shall be based on the risk assessment.

5.11.1 Stop functions

Stop functions shall override related start functions. Stop functions should be selected according to the risk assessment based on the categories listed below.

There are three categories of stops as follows:

— Category 0: stopping by immediate removal of power to the actuators which cause hazardous conditions (i.e. an uncontrolled stop, see 3.31).

— Category 1: a controlled stop (see 3.3) with power to the actuators which cause hazardous conditions available to achieve the stop and then removal of power when the stop is achieved;

— Category 2: a controlled stop with power left available to the actuators which cause hazardous conditions.

Categories 0 and 1 shall be designed in accordance with 5.3.

Each zone shall be equipped with a category 0 or 1 stop (or both) depending upon the risk assessment. Restoration of normal power after a category 0 or 1 stop shall not by itself cause hazardous conditions.

5.11.2 Emergency stop

The system shall be provided with one or more emergency stop functions which can be applied to the entire system or to clearly distinguishable zones within the system.

In the case of clearly distinguishable zones within a system, those zones should have their own emergency stop function which applies to that zone only. Where one or more zones are in an emergency stop condition, the system (or remaining portions of the system) shall be notified of the condition. After the actuation of an emergency stop device for a clearly distinguishable zone, no hazards shall exist at the interface between this zone and other areas of the system.

Where the emergency stop function is implemented by an electrical circuit, it shall be in accordance with IEC 204-1 and in accordance with EN 418 in the case of using hydraulic power for drive power.

Human intervention by designated personnel shall be required to reset the emergency stop circuit. Resetting of the emergency stop shall not initiate or restart any hazardous motions or create any hazardous conditions.

Each control station shall be provided with a manually operated emergency stop device which shall be associated with the clearly distinguishable zone. The actuators of manually-operated emergency stop devices shall be in accordance with IEC 204-1.

5.11.3 Interruption by safeguards

The safeguard (e.g. a trip device or interlocked guard) shall be connected to a stop function of category 0 or 1. The activation of these safeguards is in many cases a part of the working procedures for the system. It is therefore essential that this stop function allows an easy restart of the system or portion thereof. When this is not practicable because of the production process, then an operational stop function shall be provided which can be activated before the safeguards are activated. This operational stop function shall be designed to stop the production process at a natural point in the production process to avoid damage to the machine, product and process.

When an operational stop is provided, and where it is not possible for safety reasons to stop a process during any production cycle or part thereof, the electrically interlocked guards with guard locking shall be used for safeguarding to prevent personnel entering the hazard zone until the production cycle has ended and all hazards have been eliminated.

5.11.4 Operational stop

Operational stop functions which are category 2 stops shall be in compliance with IEC 204-1. This level of stopping is intended as a functional or operational stop and not as a safety measure.

5.12 Emergency movement

Means shall be provided to provided movement of system elements under emergency conditions. These means are for example:

a) with power off:

- — venting of relief valves to depressurize systems under pressure;
- — manual release of mechanically-actuated brakes provided that additional hazards are not created;

b) with power on:

- — manual control facilities of power-piloted valves/drives;
- — control facilities to start counter motions.

5.13 Power interruption or fluctuation

Interruption or fluctuation in any of the power sources shall not cause any hazardous situations or it shall initiate an immediate stopping action. Restoration of power by itself shall not cause any hazardous situations or restart the system.

5.14 Power disconnection

Disconnecting means for all externally supplied power sources shall be provided and marked or labelled to identify the power source. Externally supplied power sources shall have a disconnecting means with lockout capabilities.

The entire system or clearly distinguishable zones within the system shall have means to disconnect each of its power sources. These means shall be located in such a way that not person will be exposed to hazards and shall have a lockout capability.

NOTE 3 For requirements of electrical supply disconnecting devices, see IEC 240-1.

5.15 Stored energy

Means shall be provided for the isolation, containment, or controlled release of stored energy that can create a hazardous situation.

5.16 Safety related parameters

If preset limits for safety related parameters are exceeded, the control system shall initiate appropriate measures to eliminate or reduce the hazard. Examples of safety related parameters are displacement, speed, temperature, and pressure.

6 Design and safeguarding of the system

6.1 General

The following safeguards may be used for the protection of persons from hazardous situations provided they meet the requirements of 5.3:

- — fixed or movable guards;
- — trip devices used with interlocking (e.g. light beams/curtains, pressure-sensitive plates/pressure-sensitive mats, tactile sensors);
- — person location dependent safety measures (e.g. two-hand controls, enabling devices).

In addition, means such as awareness barriers, awareness devices and signals, warning signs and symbols, safety markings, and safe working practices may be used but not•as a substitute unless determined by the risk assessment.

6.2 Safeguarding requirements

This subclause specifies the requirements for the safeguarding of the system.

6.2.1 Identification of the perimeter

The perimeter of the system or zones within the system should be defined or marked. Where hazard zones occur at the perimeter, safeguarding shall be provided to prevent or detect personnel inadvertently reaching into or entering the hazard zone. Detection of entry shall prevent initiation of hazardous motions within the hazard zone or shall cause cessation of hazardous motions before personnel are exposed to the hazard.

Means provided to access the system from the perimeter shall prevent personnel from inadvertently reaching into a hazard zone.

6.2.2 Safeguarding within the system

Where a hazard, either immediate or impending, exists between individual machines or other components of the system

- guards shall be provided to prevent personnel from entering or reaching into a hazard zone, or
- trip devices shall be provided to detect personnel reaching into or entering a hazard zone.

Detection shall prevent initiation of hazardous situations, cause immediate stopping action (see 5.11.3) of hazardous situations within the hazard zone or prevent hazardous situations from entering the hazard zone.

6.2.3 Safeguarding at the individual component machines

Where personnel are exposed to hazards associated with an industrial machine or other equipment within the system, safeguarding shall be provided in accordance with the appropriate International Standard. Where such a standard does not exist, the requirements of this International Standard shall apply or additional safeguarding shall be provided.

6.2.4 Safeguarding during manual operation

Proper safeguarding shall be provided for use during setup, programming, program verification, troubleshooting, maintenance and repair operations.

During setup, maintenance, and repair operations, hazardous situations within the hazard zone(s), shall be under local control.

6.3 Guards

The following types of guards shall be considered when specifying the safeguarding of the system:

- fixed which can only be detached by the use of tools;
- movable (e.g. adjustable, insertable, reversible);
- perimeter with or without gates or points of access (e.g. material load/unload).

NOTES

4 A guard may act alone; it is then only effective when it is closed in conjunction with an interlocking device, or with an interlocking device with guard locking; in this case protection is ensured whatever the position of the guard.

5 Closed means kept in place for a fixed guard.

Fixed guards shall be kept in place

- either permanently (e.g. welding);
- or by means of fasteners (e.g. screws, nuts) making removal/opening impossible without the use of tools.

Movable guards are those connected by a mechanical means to the machine frame or adjacent fixed element, generally via hinges or slides, and which can be opened without the use of tools. They shall be interlocked to initiate stopping of hazardous conditions and prevent initiation of hazardous conditions if the guard is open.

Movable guards shall

- be located such that entry is into a nonhazardous zone;
- prevent entry into a hazard zone until hazardous conditions cease;
- when opened, prevent hazardous conditions from being initiated or cause the initiation of immediate stopping action of hazardous conditions within a hazard zone or prevent hazardous conditions from entering a hazard zone;
- not inhibit egress of personnel from the system.

Guards used to safeguard personnel from hazards associated with the system shall be designed, constructed and applied to

— prevent personnel from inadvertently reaching into or entering a hazard zone over, under, around or through the guard;

— not in or of themselves create a hazard to personnel or with other elements of the system;

— have a clearly defined protective position (e.g. by use of hinges, stops, rails);

— provide visibility into the work zone appropriate for the particular operation;

— be installed in such a manner that they are not readily removable and shall be attached to a fixed surface;

— use materials of such design and strength to protect personnel from hazards associated with the intended use of the system and withstand normal operational and environment forces.

6.4 Interlocks and protective trip devices

6.4.1 Interlocks

The interlock shall be designed and constructed in accordance with 5.1. Together with the guard with which it operates, it shall be installed and adjusted so that when in use:

— the control system through the interlock prevents the system or that portion of the system controlled by the interlock from normal operation until the guard is closed and reset where necessary (see 6.4.3);

— closing shall not initiate normal operation. Initiation shall be a deliberate action by the operator (see 5.10);

— either the guard remains locked closed until the hazard has passed (interlocking guard with guard locking) or opening the guard while the system is working gives a category 0 or category 1 stop function (interlocking guard);

— when an interlock has been reestablished, it shall be possible to restart the system or part of the system from the stopped position provided that this does not create other hazards;

— interruption of the power sources may be sufficient to eliminate the hazard before access is possible. Where the hazard cannot be eliminated immediately by power interruption, the interlocking system shall need to include a guard locking or a braking system;

— where whole body access to the safeguard space is possible and the reset device cannot be placed so that there is a good visibility for checking that no person is present within the safeguarded space additional means, which prevent restart when a person is in a safeguarded space, shall be taken;

— actuation of an interlock installed to protect against one hazard (e.g. stopping hazardous situations) does not create a different hazard, e.g. the release of hazardous substances into the work zone.

Selection of the preferred system of interlocking for a particular application shall take account of the risk assessment (see 4.5) and the frequency of opening a movable guard for access (i.e. human intervention) to the hazard zone:

— movable guards for frequent access (e.g. on operation areas for loading and unloading of products) with interlocking devices based on component duplication and/or monitoring;

— movable guards for infrequent access (e.g. to carry out adjustment or maintenance) with interlocking devices based on inherently safe design.

A guard associated with an interlocking device (interlocking guard) shall be such that

— the hazardous functions covered by the guard cannot operate until the guard is closed;

— where the guard is opened while the hazardous functions covered by the guard are operating, a stop instruction is given;

— when the guard is closed, the hazardous functions covered by the guard can operate but the closure of the guard by itself does not initiate their operation.

A guard associated with an interlocking device and a guard locking device (interlocking guard with guard locking) shall be such that

— the hazardous functions covered by the guard cannot operate until the guard is closed and locked;

— the guard remains locked closed until the risk of injury from the hazardous functions covered by the guard has passed;

— when the guard is closed and locked, the hazardous functions covered by the guard can operate but the closure of the guard does not by itself initiate their operation.

6.4.2 Protective trip devices

The following types of protective trip devices shall be considered when designing the safeguarding of the system:

— pressure sensitive mats and pads;

— electrosensitive protective devices (e.g. light beams and curtains);

— tactile sensors.

The consideration of the design shall not be limited to the above.

Protective trip devices used to protect personnel from hazards associated with the system shall

— detect personnel reaching into or entering the hazard zone through the plane or area protected by the device;

— have an identifiable minimum object sensitivity such that an object of equal or greater size or mass will be detected anywhere within the sensing field regardless of the plane of intrusion;

— be located at a distance from the hazardous condition such that the condition ceases prior to personnel reaching the hazard;

— prevent a hazardous condition from being initiated or initiate an immediate stopping action of the hazardous condition within the hazard zone or initiate stopping action of hazardous conditions before they can reach personnel;

— not in or of itself create a hazard.

Restarting of normal operation shall require that the interruption of the device shall be cleared and reset where required (see 6.4.3), and that the system is reinitiated by normal means (see 5.10).

All areas of entry into the hazard zone not protected by the device shall be protected by other safeguarding.

Muting of the device shall be permitted when it is necessary for workpieces, material or components to enter or exit a hazard zone of the system.

The device or its interface shall incorporate a means to visually indicate when it is in use, when it is functioning properly, when it is muted and when it has detected an intrusion.

The ability to detect an intrusion shall not be adversely affected by changes in the intended physical environment or normal operating conditions of the system.

Devices that require adjustments or that incorporate optional features or functions shall be designed or constructed such that these adjustments or features are capable of being supervised and/or locked.

The device shall have a maximum response time that is not adversely affected by adjustments or changes in the conditions of the intended physical environment.

Protective trip devices shall be positioned so as to prevent access to the hazard(s) until it has been eliminated or reduced to an acceptable level.

Where whole body access to the safeguarded space is possible and the reset device cannot be placed so that there is good visibility for checking that no person is present within the safeguarded space additional means, which prevent restart when a person is in a safeguarded space, shall be provided.

6.4.3 Resetting

Resetting of the interlocks and other protective devices is required where whole body access is possible. Reset shall ensure given conditions before initiating operation.

Reset shall

— ensure that all safety functions and protective devices are active;

— not initiate motion or a hazardous situation;

— be by deliberate manual action;

— prepare the machine system for all starts;

— be inoperative during the operating mode of the machine.

The manually-operated resetting device shall be located outside the hazard zone from which there is good visibility for checking that no person is present within the hazard zone.

Resetting in the safeguarded space may be allowed as an exception for the emergency stop device and the enabling device.

6.5 Enabling devices

Where an enabling device is provided as part of the system, it shall be designed to allow motion or other hazardous situation when actuated in one position only. In any other position, hazardous situations shall be stopped safely. Operation of the device by itself shall not initiate hazardous situations.

When an enabling device is required, it shall be connected to a category 0 or category 1 stop (see 5.11.1).

Enabling devices shall be designed in compliance with the ergonomic principles. A simple defeat shall be prevented.

There are two types of enabling devices as follows:

a) two-position:

   1) position 1: off-function of the switch (actuator is not pushed),

   2) position 2: enabling function (actuator is pushed);

b) three-position:

   1) position 1: off-function (actuator is not pushed),

   2) position 2: enabling function (actuator is pushed to its mid-position),

   3) position 3: off-function (actuator is pushed past its mid-position).

When returning from position 3 to position 2 the enabling function shall not become active.

Other solutions may be used where they provide an equivalent level of safety. A hold-to-run control device which meets the requirements of 5.3 may be used as an alternative to the enabling device and used for the same purposes.

6.6 Warning devices

Warning devices may be used in addition to, but not as a substitute for, safeguarding except where determined by the risk assessment.

Warning devices shall indicate or announce an impending or present hazard within the system by tactile, visual or audible means. Examples of warning devices can include but are not limited to

a) tactile

   1) curtains,

   2) chains or ropes,

   3) railings;

b) visual

   1) signs,

   2) floor markings,

   3) lights (steady, flashing, rotating);

c) audible

   1) bells,

   2) horns,

   3) whistles,

   4) sirens.

Warning devices shall be designed, constructed and installed such that they shall provide a distinguishable indication (e.g. flashing light) of an impending or present hazard.

NOTE 6 For the use and frequency of flashing lights, see IEC 73.

6.7 Safety markings

Safety markings (e.g. signs, symbols, labels, warning paint) shall be of a durable material, easy to understand, represent a contrast to the surrounding background and applied in a durable manner. See also ISO 3864.

Safety signs should be applied where additional indication of a potential hazard (e.g. existing remaining energies, and to mark protected areas) is required.

6.8 Safe working procedures

It is recognized that for certain phases of the system life (e.g. commissioning, process changeover, cleaning and maintenance) it may not be practicable to design completely adequate safeguards to protect against every hazard especially where certain safeguards may be suspended. For such conditions, appropriate safe working procedures shall, as far as possible, be addressed in the manual.

6.9 Openings for loading and unloading of material

6.9.1 General

This subclause applies to openings provided for the passing of material into or out of the system which are small enough to prevent entrance of persons. Where these openings are large enough to allow the entrance of persons, the requirements of 6.2 shall apply.

6.9.2 Manual loading and unloading

Personnel shall not be exposed to hazardous situations during manual loading and unloading of workpieces of parts.

6.9.3 Automatic loading and unloading

Personnel shall not reach hazardous points or areas when automatic loading and unloading takes place and they shall not be exposed to hazardous conditions.

6.10 Stopping time/distance

When relevant, the supplier shall state the stopping time or distance (or both).

7 Training, installation, commissioning and functional testing

7.1 General

This clause contains provisions and requirements for training of personnel and installing and functional testing the system prior to its use in normal operation.

7.2 Training

Instructions as necessary for the safe use of the integrated manufacturing system shall be established.

The user shall ensure that personnel who program, operate, maintain or repair the systems are adequately trained and demonstrate competence to perform their tasks safely. Training shall include, but not be limited to

a) a review of applicable standard safety procedures and the safety recommendations of the suppliers of the system and its component elements;

b) a clear definition of assigned tasks;

c) identification and explanation of all control devices and their functions used in performing the assigned tasks;

d) identification and clarification of lockout procedures;

e) identification of the hazards associated with the assigned tasks;

f) the method(s) of safeguarding (including the safe working procedures) from the identified hazards;

g) the method for functional testing or otherwise ensuring the proper functioning of the safeguards;

h) the method for testing or otherwise ensuring the proper functioning of the safeguards and interlocks.

7.3 Installation

The system shall not be installed in accordance with the manufacturer's requirements with the safeguarding methods identified by the hazard analysis and the risk assessment. The user shall review the safety requirements to ensure that the appropriate safeguards are applied prior to commissioning.

When the safeguarding methods are not in place prior to commissioning and functional testing, interim means of designating (e.g. markings, awareness barriers, warning signs) the hazard zones shall be in place before proceeding.

7.4 Commissioning and functional testing

7.4.1 Commissioning

The safety requirements shall be reviewed to ensure that appropriate safeguards are in place prior to commissioning.

Where integrated manufacturing systems, sections of systems or single units are installed and tested and the required safety measures for the particular modes of operation according to this International Standard are not practicable, the following requirements (as a minimum) shall apply:

— the necessary safety measures shall be determined and implemented;

— only authorized personnel are allowed in hazard zones;

— emergency stop function shall be active;

— designate (e.g. mark, awareness barriers, warning signs) the hazard zones;

— the locking devices to prevent unintended operation (e.g. keys, padlocks);

— provide personal protective equipment and ensure their use;

— provide means for rescue (see 5.12).

7.4.2 Functional testing

The manufacturer's instructions for functional testing of the system shall be followed. An initial start-up procedure shall include, but not necessarily limited to, the following:

a) before applying power, verify that

1) the system including its individual machines and associated equipment has been properly mounted and is stable,

2) the electrical connections are correct and that the power (i.e. voltage, frequency, interference levels) is within specified limits,

3) the other utilities (e.g. water, air, gas) are properly connected, identified and within specified limits,

4) the peripheral equipment is properly connected,

5) the limiting devices that establish the restricted space (when utilized) are installed,

6) the safeguarding means are applied,

7) the physical environment is as specified (e.g. lighting and noise levels, temperature, humidity, atmospheric contaminants);

after applying power, verify that

1) it is possible to disconnect and isolate the external power sources,

2) other safeguarding methods are in place (e.g. awareness barriers, warning devices),

3) the safeguards and interlocks function as intended,

4) the start, stop and mode selection (including the key lock switches) control devices function as intended,

5) each individual machines moves and is restricted as intended,

6) the teach and data retention functions operate correctly,

7) in reduced speed mode (where applicable), the system or portion of the system which is being functionally tested operates properly and has the capability to handle the product or workpiece,

8) in normal operation, the system operates properly and has the capability to perform the intended task(s) at rated performance.

8 Use and care

8.1 General

This clause specifies the requirements for safety during normal and manual operations.

8.2 Requirements for personnel

Only personnel having been properly trained concerning the hazards and safety measures of the system shall be assigned to work with the system, zones of the system and individual machines.

8.3 Normal operation

The initiation of normal operation for the complete system, sections of system, or individual machines shall only be allowed where all of the following conditions are satisfied:

— the normal operation mode has been selected (see 5.7);

— the associated safeguards are in place and functioning (not suspended);

— no persons are present within the safeguarded space; and

— proper safe working procedures are followed.

Before returning to normal operation from any other mode of operation as described below, all of the above conditions shall be satisfied.

The initiation of hazardous situations should be announced by warning signals (acoustic or visual). Where necessary, appropriate mesures shall be taken to ensure that all persons have left the hazard zone(s).

8.4 Manual operation

Manual operations (e.g. setup, programming, program verification, troubleshooting, maintenance and repair, and fault elimination) shall be performed from outside the safeguarded space wherever practicable with the safeguarding requirements described in 6.2 maintained.

When it is necessary to perform manual operations with personnel inside the safeguarded space, the protective effectiveness of the safeguards (e.g. door interlocking, presence sensing devices) may be suspended by means of selection of operating conditions according to 5.7 and 5.8 provided that additional means of safeguarding as determined by the risk assessment are provided.

When it is necessary for personnel to enter the safeguarded space to perform manual operations, additional safety measures (as described in 5.8) shall be provided. This includes the initiation of motion at speeds in accordance with 5.4.1 and speeds greater than those allowed by 5.4.1. All persons required to be in the safeguarded space during manual operations shall be provided with the appropriate safety measures.

8.4.1 Safety measures for reduced speed operation

Where the reduced speed is in accordance with 5.4.1, hazardous movement shall be controlled by

a) hold-to-run according to 5.3 and emergency stop; or

b) 3-position enabling device (see 6.5); or

c) 2-position enabling device (see 6.5) and emergency stop.

Where the reduced speed does not fulfil the requirements of 5.3, only b) or c) above shall be provided.

Other solutions are possible if the same safety level is achieved.

8.4.2 Safety measures for non-reduced speed operation

a) Programming and set-up (setting)

When it is permitted to initiate hazardous motions at speeds greater than reduced speed, motion shall only be allowed with the use of a fixed hold-to-run control together with an emergency stop located such that the programmer cannot operate it when exposed to hazards.

b) Program verification and troubleshooting

Where the speed does not fulfil the requirements of 5.4.1, motion shall only be allowed with the use of either

— a three-position enabling device (see 6.5); or

— a two-position enabling device (see 6.5) and emergency stop; or

— a protective device which ensures that the person is in a nonhazardous area (e.g. use of two-hand control).

Table 1 — Summary of possible safety measures when personnel are inside the safeguarded space

Type of manual operation	Relevant subclause	
	Reduced speed in accordance with 5.4.1	Speed not in accordance with 5.4.1
Setup	8.4.1	8.4.2 a)
Programming	8.4.1	8.4.2 a)
Program verification	8.4.1	8.4.2 b)
Troubleshooting	8.4.1	8.4.2 b)

8.5 Programming

Where practicable, programming shall only be done with reduced speed (see 8.4).

Wherever possible, a record of the task programs together with any modifications should be maintained.

Programmed data that is stored on a transportable media (e.g. paper, magnetic) shall be stored in a suitably protected environment when not in use.

8.5.1 Prior to programming

The programmer shall be required to select the programming mode of operation prior to entering the safeguarded space. Automatic operation shall not be possible.

The programmer shall visually check the system and the safeguarded space to ensure that extraneous conditions which can cause hazards do not exist.

8.5.2 During programming

During programming, only the programmer shall be allowed in the safeguarded space and the following conditions shall be met:

- the system or portion of the system to be programmed shall be under the sole control of the programmer within the safeguarded space;
- the controls of the pendant shall be used as intended;
- the system or portions of the system to be programmed shall not respond to any remote commands or conditions that would cause hazardous situations;
- movement of other equipment in the safeguarded space which can present a hazard shall either be prevented or under the sole control of the programmer. When under control of the programmer, it shall require deliberate action on the part of the programmer separate from the action to initiate motion;
- all emergency stop devices shall remain functional.

8.6 Program verification

Program verification shall initially be performed at reduced speed (see 8.4).

When in exceptional cases it is necessary to examine the movement of the system or portions of the system at full (operational) speed (or any other speed that does not meet the requirements of 5.4.1) and one or more of the safeguards are suspended, it shall only be allowed through actuation of a key switch that cancels the reduced speed.

The conditions of 8.4.2 b) shall apply.

8.7 Troubleshooting and observation of production cycle

Troubleshooting shall be performed according to the information in the operating instructions and the instruction manual.

When troubleshooting requires observation of production cycles at operational speed with one or more of the safeguards suspended, it shall only be possible through the actuation of a key-operated switch or by other devices with an equivalent level of safety.

The conditions of 8.4.2 b) shall apply.

8.8 Maintenance and repair

The system shall have a inspection and maintenance procedures to ensure continued intended operation of the system. The inspection and maintenance programme shall take into account the recommendations of the system supplier and those of suppliers of various elements of the system.

Personnel who perform maintenance or repairs on the system shall be trained in the procedures necessary to perform the required tasks.

Wherever practicable, maintenance and repair shall be performed from outside the hazard zone by positioning the individual machines and associated equipment in predetermined positions.

When it is necessary to perform maintenance and repair within the hazard zone, all energy sources which can cause hazardous situations should be isolated using a lockout procedure which includes provisions for energy dissipation.

For protection against hazards coming from adjoining sections of the system or single units, additional safeguards shall be provided as well as safety measures as they are required for manual mode (see 5.7).

8.9 Fault elimination

Where fault elimination is necessary from inside the safeguarded space, it shall be performed after safe disconnection (if possible lockout). Additional measures against erroneous initiation of hazardous situations shall be taken.

Where hazards can occur during fault elimination at sections of the system or at the machines of adjoining systems or machines, these shall also be taken out of operation and protected against unexpected starting.

By means of instruction and warning signs, attention shall be drawn to fault elimination at systems which cannot be observed completely.

8.10 System restart procedures after maintenance and repair

A procedure for initiating normal operation of the system (or portion of the system which has been modified) after hardware, software or task program modification, repair or maintenance shall include but not necessarily be limited to the following:

- Check any changes or additions to the hardware prior to applying power.

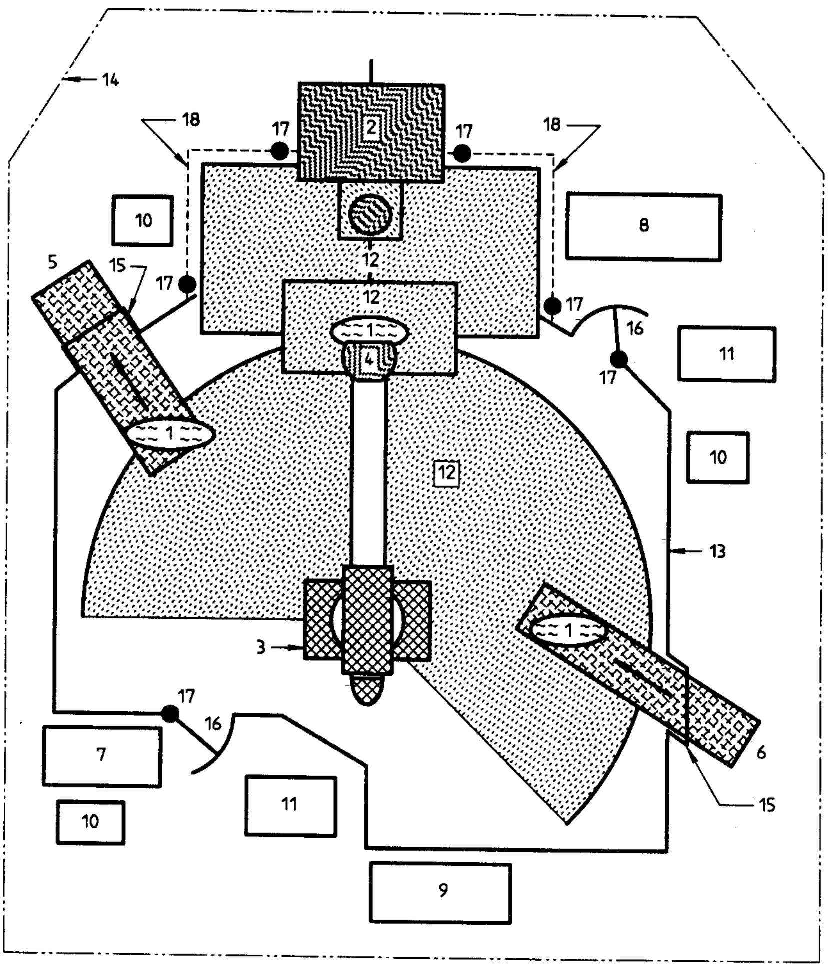
— Functionally test the system (or portion of the system which has been modified) for proper operation.

Initiation of normal operation shall require that all personnel have exited the hazard zone, the safeguards are functional and returned to their protective positions and reset, and the system is reinitiated by the normal actuating means (see 8.3).

Annex A
(informative)

Examples of a typical integrated manufacturing system

Figures A.1, A.2 and A.3 show examples of typical integrated manufacturing systems.



1 — Workpiece
2 — Machine tool
3 — Robot
4 — End effector
5 — Unload station
6 — Load station
7 — System controller
8 — Machine tool control system
9 — Robot control system
10 — Emergency stop device
11 — Warning device
12 — Hazard zone
13 — Barrier with interlocked gates
14 — Perimeter identification (marking or barrier)
15 — Movable guard or electrosensitive protective device
16 — Interlocked gate
17 — Interlocking device
18 — Barrier or electrosensitive protective device

Figure A.1 — Simple integrated manufacturing system showing perimeter identification, fixed guard with movable interlocked guards (barrier with interlocked gates), presence sensing devices, and warning devices

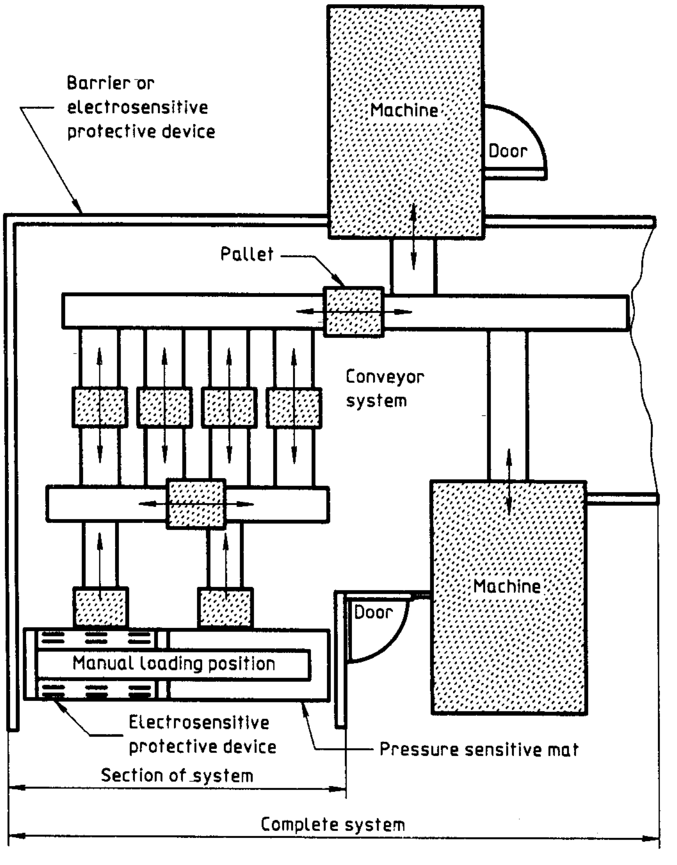


Figure A.2 — Complete system, section of system and machines

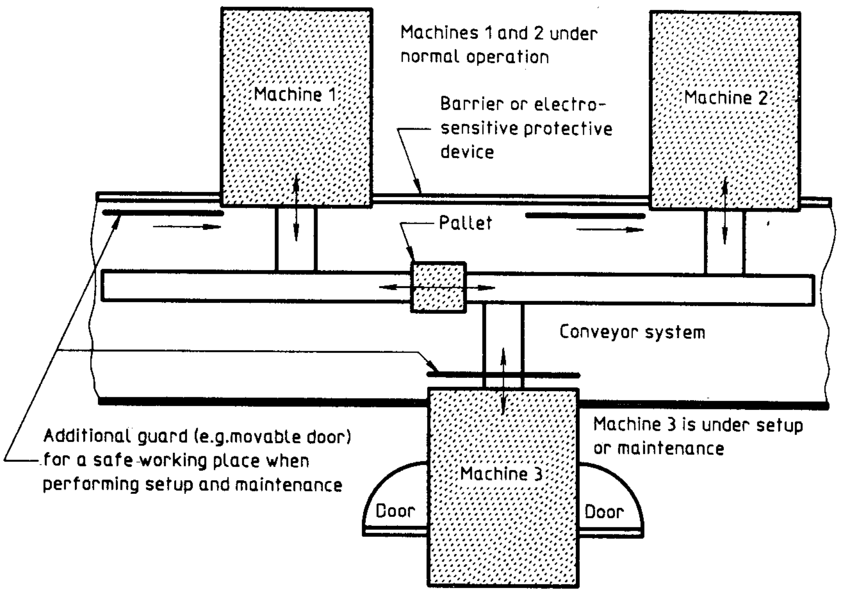


Figure A.3 — Example of additional safety measures for setup and maintenance activities

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc: No. BP 18 (0302).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 323 01 31, 323 3375, 323 94 02

Telegrams: Manaksanstha
(Common to all offices)

Regional Offices:		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	323 76 17, 323 38 41
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	337 84 99, 337 85 61 337 86 26, 337 91 20
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160022	60 38 43 60 20 25
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	254 12 16, 254 14 42 254 25 19, 254 13 15
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	832 92 95, 832 78 58 832 78 91, 832 78 92

Branches : AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.

Printed at Simco Printing Press, Delhi